RECEIVED
CENTRAL FAX CENTER
AUG 17 2007

REMARKS

Claims 13-16 are all the claims pending in the application.

I. Claim Rejections under 35 U.S.C. § 103(a)

Claims 13-16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneck et al. (U.S. 6,314,409) in view of Maytas et al. (U.S. 5,200,999). Applicants respectfully traverse this rejection on the following basis.

A. Claim 13

Regarding claim 13, Applicants note that this claim recites the feature of a cryptographic processing means that restrains the result of cryptographic processing from being outputted when a notification signal indicates that key generation is being performed. Applicants respectfully submit that the combination of Schneck and Maytas does not disclose or suggest such a feature.

In the Office Action, the Examiner has taken the position that Fig. 10A of Schneck discloses the above-noted feature recited in claim 13 (see lines 5-7 on page 3 of the Office Action). Applicants respectfully disagree.

Regarding Schneck, Applicants note that Schneck discloses a digital data access and distribution system 100 which includes a data distributor 102 and a user 104 (see Fig. 1 and col. 9, lines 51-55). As shown in Fig. 1, the data distributor 102 includes an authorizing mechanism 112, and the user 104 includes an access mechanism 114.

As explained in Schneck, data-encrypting keys K_D are generated in a typical manner suitable for a selected data-encrypting algorithm, with the data-encrypting keys K_D being used for the transfer of data between the distributor 102 and the user 104 (see col. 12, lines 13-38 and 54-55).

With respect to Fig. 10(a) of Schneck, which was relied upon by the Examiner in the Office Action, Applicants note that this figure relates to an accessing operation performed by the access mechanism 114 of the user device 104, wherein the user 104 obtains packaged data 108 from the distributor 102 and accesses the data according to the rules provided therewith (see col. 17, lines 46-52).

In particular, as explained with reference to Fig. 10(a) of Schneck, it is determined whether a data element is protected (step S1012), wherein if the data element is determined to be protected, then it is next determined whether access to the data element is permitted (step S1014). If access is permitted, then the data element is made available (step S1018), and if no access is permitted, then an access denial operation is performed (step S1016) (see col. 18, lines 44-59).

Thus, while Fig. 10(a) of Schneck depicts the ability to determine whether access to a data element is permitted or not, and deny access if it is determined that access is not permitted (step S1016), Applicants respectfully submit that such disclosure does not in any way whatsoever correspond to the ability to restrain the result of cryptographic processing from being outputted when a notification signal indicates that key generation is being performed, as recited in claim 13.

In other words, while Schneck discloses the ability to deny access to a data element, Applicants note that Schneck does not disclose or even remotely suggest that there is any type of relationship between the denial of access and the above-noted generation of the data encrypting keys K_D.

As such, contrary to the position taken by the Examiner in the Office Action, Applicants respectfully submit that Schneck does not disclose, suggest or otherwise render obvious at least the above-noted feature recited in claim 13 of a cryptographic processing means that restrains the result of cryptographic processing from being outputted when a notification signal indicates that key generation is being performed.

Further, Applicants respectfully submit that Maytas fails to cure this deficiency of Schneck. In particular, regarding Maytas, Applicants note that this reference discloses a cryptographic facility (CF) 30 in which a public key (PU) and a private key (PR) are generated, with the keys being formatted in a PU key record and a PR key record (see col. 13, lines 40-50). In this regard, as explained in Maytas, the PU and PR key records are encrypted while generating the PU and PR key records (see col. 13, lines 36-50 and col. 18, lines 57-63).

As pointed out by the Examiner in the Office Action, Maytas disclose a procedure for generating the above-noted PU key and PR key at col. 87, line 20 through col. 89, line 25. In this regard, as explained in Maytas, step 1 of this procedure is performing input parameter consistency checking (see col. 87, line 63), step 2 is performing configuration vector and state vector checking (see col. 88, lines 22-23), step 3 is performing control block and control vector checking, and step 4 is generating the PU key and the PR key (see col. 88, line 43).

In Maytas, regarding the generation of the PU key and the PR key, it is disclosed therein that the generation of these keys can only be executed when the CF STATE is in the "run state", with the CF STATE being a state vector that indicates the state of the cryptographic facility 30 (see col. 29, lines 64-66; col. 87, lines 60-61 and col. 88, lines 24-25).

Thus, in Maytas, the cryptographic facility (CF) 30 produces the PU key and PR key which are formatted in a PU key record and PR key record, encrypts the produced PU key and PR key records, and outputs the encrypted PU key and PR key records, wherein the state of the cryptographic facility (CF) 30 is indicated by the CF-STATE, and only when the CF-STATE is in the "run" state are the PU key and PR key records output from the cryptographic facility (CF) 30, with a control vector being able to block the output of the PU key and PR key records.

Based on the foregoing description of Maytas, as well as the above-noted description of Schneck, Applicants note that if these two references were somehow combined, that such a combination would result in, at best, the data processing of the cryptographic facility (CF) 30 of Maytas being applied to the data-encrypting key K_D of Schneck, with the control vector of Maytas being able to block the outputting of the data-encrypting key K_D of Schneck.

In contrast, according to claim 13, the output of the cryptographic processing is restrained based on a notification signal which indicates that key generation is being performed. Applicants respectfully submit that the combination of Maytas and Schneck does not teach or in any way suggest such a feature.

Instead, as noted above, Applicants submit that such a combination would, at best, result in a system in which the control vector of Maytas was able to block the outputting of the data-encrypting key K_D of Schneck. The mere ability to block the output of a data-encrypting key,

however, does not in any way whatsoever correspond to the ability to restrain the output of cryptographic processing based on a notification signal which indicates that key generation is being performed, as recited in claim 13.

In view of the foregoing, Applicants respectfully submit that the combination of Schneck and Maytas does not teach, suggest or otherwise render obvious all of the features recited in claim 13. Accordingly, Applicants submit that claim 13 is patentable over the cited prior art references, an indication of which is kindly requested.

B. Claim 14

Regarding claim 14, Applicants note that this claim recites the features of key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not, and selection means for selecting a content which is inputted to the cryptographic processing means when the notification signal indicates that key generation is being performed, and otherwise selecting the result of the cryptographic processing outputted from the cryptographic processing means.

Applicants respectfully submit that the combination of Schneck and Maytas does not teach or suggest at least the above-noted features recited in claim 14.

In particular, as discussed with respect to claim 13, Schneck discloses the ability to generate a data-encrypting key K_D, and Maytas discloses the ability to utilize a control vector in order to block the output of the PU key and PR key records. As such, Applicants submit that even if these two references were somehow combined, that such a combination would merely result in a system in which the control vector of Maytas was able to block the outputting of the data-encrypting key K_D of Schneck.

In this regard, Applicants submit that the mere ability to block the output of a data-encrypting key does not in any way whatsoever correspond to the ability recited in claim 14 of

selecting a content which is inputted to the cryptographic processing means when the notification signal indicates that key generation is being performed, and otherwise selecting the result of the cryptographic processing outputted from the cryptographic processing means.

Indeed, in the Office Action, Applicants note that the Examiner has not identified any passages or elements in either Schneck or Maytas which allegedly correspond to the above-noted feature recited in claim 14. Instead, the Examiner has merely stated that claim 14 is rejected for a least the same reasons as claim 15.

In view of the foregoing, Applicants respectfully submit that the combination of Schneck and Maytas does not teach, suggest or otherwise render obvious at least the above-noted features recited in claim 14. Accordingly, Applicants submit that claim 14 is patentable over the cited prior art references, an indication of which is kindly requested.

If the Examiner maintains the rejection of claim 14, Applicants request that the Examiner explicitly identify the elements and passages of Schneck and Maytas that are being relied upon as allegedly corresponding to each of the features recited therein, so that Applicants may make an informed decision with regard to appeal.

C. Claim 15

Regarding claim 15, Applicants note that this claim recites the features of a cryptographic processing means which outputs to an input means an input enable signal indicating either one of an input enabled state in which inputting of the content from the input means is enabled and an input disabled state in which inputting of the content from the input means is disabled, wherein, when a notification signal output by a key generation means indicates that key generation is being performed, the cryptographic processing means outputs to the input means the input enable signal indicating the input disabled state, and wherein the input means disables outputting of the inputted content when the input enable signal indicates the input disabled state. Applicants respectfully submit that the combination of Schneck and Maytas does not teach or suggest such features.

In the Office Action, the Examiner has acknowledged that Schneck does not disclose any of the above-noted features, but has taken the position that the disclosure in Maytas at col. 87, line 20 through col. 89, line 25 cures these deficiencies of Schneck. Applicants respectfully disagree.

In particular, as discussed above with respect to claim 13, Applicants note that the disclosure in Maytas at col. 87, line 20 through col. 89, line 25 relates to the generation of a PU key and PR key, wherein a control vector that is input to the cryptographic facility (CF) 30 can be utilized to block the outputting of these keys.

Thus, while Maytas discloses the use of a control vector which can be used to block the outputting of the PU key and the PR key, Applicants respectfully submit that such disclosure does not in any way whatsoever correspond to the above-noted features recited in claim 15 of a cryptographic processing means which outputs to an input means an input enable signal indicating either one of an input enabled state in which inputting of the content from the input means is enabled and an input disabled state in which inputting of the content from the input means is disabled, wherein, when a notification signal output by a key generation means indicates that key generation is being performed, the cryptographic processing means outputs to the input means the input enable signal indicating the input disabled state, and wherein the input means disables outputting of the inputted content when the input enable signal indicates the input disabled state.

Accordingly, Applicants submit that claim 15 is patentable over the cited prior art, an indication of which is kindly requested.

If the Examiner maintains the rejection, Applicants kindly request that the Examiner explicitly identify the elements in Maytas which allegedly correspond to each of the above-noted features recited in claim 15 so that Applicants may make an informed decision with regard to appeal. In particular, Applicants request that the Examiner identify the elements in Maytas which allegedly correspond to the "cryptographic processing means", the "input means", the "input enable signal", the "key generation means" and the "notification signal".

Further, as discussed with respect to claim 13, regarding the Examiner's proposed combination of Schneck and Maytas, Applicants note that Schneck discloses the ability to generate a data-encrypting key K_D, and Maytas discloses the ability to utilize a control vector in order to block the output of the PU key and PR key records. As such, even if these two references were somehow combined, Applicants submit that such a combination would merely result in a system in which the control vector of Maytas was able to block the outputting of the data-encrypting key K_D of Schneck.

In view of the foregoing, Applicants respectfully submit that the combination of Schneck and Maytas does not teach, suggest or otherwise render obvious at least the above-noted features recited in claim 15. Accordingly, Applicants submit that claim 15 is patentable over the cited prior art references, an indication of which is kindly requested.

D. Claim 16

Regarding claim 16, Applicants note that this claim recites the features of a key generation means which outputs to an input means an input enable signal indicating either one of an input enabled state in which inputting of the content to the cryptographic processing means is enabled and an input disabled state in which inputting of the content to the cryptographic processing means is disabled, wherein, when key generation is being performed, the key generation means outputs to the input means the input enable signal indicating the input disabled state, and wherein the input means disables outputting of the inputted content when the input enable signal indicates the input disabled state. Applicants respectfully submit that the combination of Schneck and Maytas does not teach or suggest such features.

In the Office Action, the Examiner has acknowledged that Schneck does not disclose any of the above-noted features, but has taken the position that the disclosure in Maytas at col. 87, line 20 through col. 89, line 25 cures these deficiencies of Schneck. Applicants respectfully disagree.

In particular, as discussed above with respect to claim 13, Applicants note that the disclosure in Maytas at col. 87, line 20 through col. 89, line 25 relates to the generation of a PU

key and PR key, wherein a control vector that is input to the cryptographic facility (CF) 30 can be utilized to block the outputting of these keys.

Thus, while Maytas discloses the use of a control vector which can be used to block the outputting of the PU key and the PR key, Applicants respectfully submit that such disclosure does not in any way whatsoever correspond to the above-noted features recited in claim 16 of a key generation means which outputs to an input means an input enable signal indicating either one of an input enabled state in which inputting of the content to the cryptographic processing means is enabled and an input disabled state in which inputting of the content to the cryptographic processing means is disabled, wherein, when key generation is being performed, the key generation means outputs to the input means the input enable signal indicating the input disabled state, and wherein the input means disables outputting of the inputted content when the input enable signal indicates the input disabled state.

Accordingly, Applicants respectfully submit that claim 16 is patentable over the cited prior art, an indication of which is kindly requested.

If the Examiner maintains the rejection, Applicants kindly request that the Examiner explicitly identify the elements in Maytas which allegedly correspond to each of the above-noted features recited in claim 16 so that Applicants may make an informed decision with regard to appeal. In particular, Applicants request that the Examiner identify the elements in Maytas which allegedly correspond to the "cryptographic processing means", the "input means", the "input enable signal", the "key generation means" and the "notification signal".

Further, as discussed with respect to claim 13, regarding the Examiner's combination of Schneck and Maytas, Applicants note that Schneck discloses the ability to generate a data-encrypting key K_D, and Maytas discloses the ability to utilize a control vector in order to block the output of the PU key and PR key records. As such, even if these two references were somehow combined, Applicants submit that such a combination would merely result in a system in which the control vector of Maytas was able to block the outputting of the data-encrypting key K_D of Schneck.

RECEIVED
CENTRAL FAX CENTER
AUG 17 2007

In view of the foregoing, Applicants respectfully submit that the combination of Schneck and Maytas does not teach, suggest or otherwise render obvious at least the above-noted features recited in claim 16. Accordingly, Applicants submit that claim 16 is patentable over the cited prior art references, an indication of which is kindly requested.

II. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Mutsuyuki OKAYAMA et al.

By: Kenneth W. Fields

Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/jjv
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
August 17, 2007